ABSTRACT

A system and method for employing a key exchange key to facilitate secure communication is provided. The key exchange key can be employed, for example, to encrypt and/or decrypt dialog session key(s) that are used to encrypt and/or decrypt message(s) that form a dialog between an initiator system and target system. In one example, a key exchange key is unique to a service pair, while a dialog session key is unique to a particular dialog between the service pair.

The system can facilitate end-to-end encryption of message data in a dialog -- the message data is encrypted at one dialog endpoint and not decrypted until it reaches the other dialog endpoint. The system can be employed to facilitate secure dialog with minimal performance overhead when compared with conventional system(s). Optionally, the system can facilitate load balancing (*e.g.,* among deployed instances of a service). In this example, secured dialogs to a service can be location transparent so that a dialog targeted to a service can be able to talk to any instance of the same service transparently without any additional security setup.

The system employs both public key/private key asymmetric encryption technique(s) and symmetric encryption technique(s) to authenticate and secure information exchanged between an initiator system and a target system.